

PATENT  
Customer No. 22,852  
Attorney Docket No. 09812.0590-00000

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re Application of: )  
)  
Taizo SHIRAI et al. )  
) Group Art Unit: 2137  
Application No.: 09/982,711 )  
) Examiner: Nadia Khoshnoodi  
Filed: October 18, 2001 )  
) Confirmation Number: 8666  
For: INFORMATION RECORDING DEVICE, )  
INFORMATION PLAYBACK DEVICE, )  
INFORMATION RECORDING MEDIUM, )  
INFORMATION RECORDING METHOD, )  
INFORMATION PLAYBACK METHOD, )  
AND PROVIDING MEDIUM )

**Mail Stop Appeal Brief--Patents**

Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

Sir:

**TRANSMITTAL OF APPEAL BRIEF (37 C.F.R. 41.37)**

Transmitted herewith is the APPEAL BRIEF in this application with respect to the  
Notice of Appeal filed on July 26, 2006.

This application is on behalf of

☐ Small Entity      ☒ Large Entity

Pursuant to 37 C.F.R. 41.20(b)(2), the fee for filing the Appeal Brief is:

☐ \$250.00 (Small Entity)

☒ \$500.00 (Large Entity)

TOTAL FEE DUE:

Appeal Brief Fee      \$500.00



Application No.: 09/982,711  
Attorney Docket No. 09812.0590-00000


Extension Fee (if any)      \$0  
Total Fee Due                      \$500.00

☒ Enclosed is a check for \$500.00 to cover the above fees.

PETITION FOR EXTENSION. If any extension of time is necessary for the filing of this Appeal Brief, and such extension has not otherwise been requested, such an extension is hereby requested, and the Commissioner is authorized to charge necessary fees for such an extension to our Deposit Account No. 06-0916. A duplicate copy of this paper is enclosed for use in charging the deposit account.

FINNEGAN, HENDERSON, FARABOW,  
GARRETT & DUNNER, L.L.P.

Dated: September 26, 2006

By:   
Arthur A. Smith  
Reg. No. 56,877



PATENT  
Customer NO. 22,852  
Attorney Docket No. 09812.0590-00000

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: )  
Taizo SHIRAI et al. ) Group Art Unit: 2137  
Application No.: 09/982,711 ) Examiner: Nadia Khoshnoodi  
Filed: October 18, 2001 ) Confirmation No.: 8666  
For: INFORMATION RECORDING DEVICE, )  
INFORMATION PLAYBACK DEVICE, )  
INFORMATION RECORDING MEDIUM, )  
INFORMATION RECORDING METHOD, )  
INFORMATION PLAYBACK METHOD, )  
AND PROVIDING MEDIUM )

**Attention: Mail Stop Appeal Brief-Patents**  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

Sir:

**APPEAL BRIEF UNDER BOARD RULE § 41.37**

In support of the Notice of Appeal filed July 26, 2006, and further to Board Rule 41.37, Appellants presents this brief and enclose herewith a check for the fee of \$500.00 required under 37 C.F.R. § 41.20(b)(2).

This Appeal responds to the April 26, 2006, final rejection of claims 1-32 under 35 U.S.C. § 103(a).

If any additional fees are required or if the enclosed payment is insufficient, Appellants request that the required fees be charged to Deposit Account No. 06-0916.

09/27/2006 SDENB081 00000033 09982711

01 FC:1402

500.00 QP

I. REAL PARTY IN INTEREST

SONY Corporation is the real party in interest.

II. RELATED APPEALS AND INTERFERENCES

There are currently no other appeals or interferences, of which Appellants, Appellants' legal representative, or Assignee are aware, that will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

III. STATUS OF CLAIMS

Claims 2-4, 7, 9-11, 14, 18-20, 23, 25-27, and 30 are canceled. Claims 1, 5, 6, 8, 12, 13, 15-17, 21, 22, 24, 28, 29, 31, and 32 remain pending and under examination. Appellants appeal the rejection of claims 1, 5, 6, 8, 12, 13, 15-17, 21, 22, 24, 28, 29, 31, and 32.

IV. STATUS OF AMENDMENTS

The Request for Reconsideration filed on June 12, 2006, did not propose any changes to the claims in this Appeal. An amendment after final, filed at the same time as this Appeal Brief, cancels claims 2-4, 7, 9-11, 14, 18-20, 23, 25-27, and 30.

V. SUMMARY OF CLAIMED SUBJECT MATTER

The claimed subject matter on appeal prevents electronic data, such as music data, video data, or software programs from being illegally copied. A memory has a data storage area divided into a plurality of blocks. Each block is divided into sectors, and a different encryption key encrypts each sector.

Independent claim 1 recites an information recording device (Fig. 2, element 200) for executing processing which stores data to a memory (*Specification*, p. 24, lines 7-21). The memory having a data storage area (Fig. 2, element 212 and 232) consisting of a plurality of blocks (Fig. 3a), each of the blocks consists of M sectors (Fig. 3b) from a first sector to a M-th sector with each sector having a predetermined data capacity where M represents a natural number (*Specification*, p. 27, lines 1-7). The information recording device comprising a cryptosystem unit (Fig. 4, element 320) that selectively uses a different encryption key for each sector from the first sector to the M-th sector to execute encryption processing and the cryptosystem unit executes encryption processing on data to be stored in each of the sectors (*Specification*, p. 80, line 16 - p. 82, line 11). Wherein the data includes a revocation list having revocation information regarding revoked media or content (*Specification*, p. 43, lines 5-23 and p. 85, lines 1-6) and a block permission table for accessing a permission table that describes memory access control information (*Specification* p. 46, lines 2-12). An integrity checking unit for checking the integrity of the revocation list and the block permission table (*Specification*, p. 51, line 18 - p. 52, line 12).

Independent claim 8 recites an information playback device (Fig. 2, element 200) for executing processing which reads data from a memory (*Specification*, p. 24, lines 7-21). The memory having a data storage area (Fig. 2, element 212 and 232) consisting of a plurality of blocks (Fig. 3a), each of the blocks consists of M sectors (Fig. 3b) from a first sector to a M-th sector with each sector having a predetermined data capacity, where M represents a natural number (*Specification*, p. 27, lines 1-7). The information playback device comprising a cryptosystem unit (Fig. 4, element 320) which selectively

uses a different decryption key for each sector from the first sector to the M-th sector to execute decryption processing and the cryptosystem unit executes decryption processing on data stored in each of the sectors (*Specification*, p. 103, line 6 - p. 105 line 17). Wherein the data includes a revocation list having revocation information regarding revoked media or content (*Specification*, p. 95, lines 10-18) and a block permission table for accessing a permission table that describes memory access control information (*Specification*, p. 100, line 23 - p. 101, line 8). An integrity checking unit for checking the integrity of the revocation list and the block permission table (*Specification*, p. 95, line 12 - p. 96, line 11).

Independent claim 15 recites an information recording medium (Fig 2, elements 210 and 230) having a data storage area consisting of a plurality of blocks (*Specification* p. 26, lines 16-24). Each of the blocks consists of M sectors from a first sector to a M-th sector with each sector having a predetermined data capacity, where M represents a natural number (*Specification*, p. 27, lines 1-7). Wherein a plurality of different cryptographic keys which are selectable for the sectors are stored as header information of data stored in said data storage area, (*Specification*, p. 36, line 18 - p. 38, line 21 and p. 40, line 1 - p. 41, line 4). Wherein the storage area stores data including a revocation list having revocation information regarding revoked media or content (*Specification*, p. 43, lines 5-23) and a block permission table for accessing a permission table that describes memory access control information (*Specification* p. 46, lines 2-12). Wherein an integrity check of the integrity of the revocation list and block permission table is performed (*Specification*, p. 51, lines 18-24).

Independent claim 17 recites an information recording method (Figs. 41 and 42) for executing processing which stores data to a memory having a data storage area consisting of a plurality of blocks, each of the blocks consists of M sectors from a first sector to a M-th sector with each sector having a predetermined data capacity, where M represents a natural number (*Specification*, p. 108, lines 7-10 and p. 112, lines 13-24). The information recording method comprising encryption processing data to be stored in the sectors by performing encryption using a different encryption key for each sector from the first sector to the M-th sector (*Specification*, p. 108, lines 7-13). Storing data including a revocation list having revocation information regarding revoked media or content (*Specification*, p. 106, line 11 - p. 107, line 15) and a block permission table for accessing a permission table that describes memory access control information (*Specification*, p. 113, lines 2-10). Performing an integrity check of the revocation list and the block permission table (*Specification*, p. 113, lines 11-16).

Independent claim 24 recites an information playback method (Figs. 35 and 36) for executing processing which reads data from a memory having a data storage area consisting of a plurality of blocks, each of the blocks consists of M sectors from a first sector to a M-th sector with each sector having a predetermined data capacity, where M represents a natural number (*Specification*, p. 93, lines 10-21). The information playback method comprising decrypting data stored in each of the sectors by executing decryption processing using a different decryption key for each sector from the first sector to the M-th sector (*Specification*, p. 96, lines 19-25). Storing data including a revocation list having revocation information regarding revoked media or content (*Specification*, p. 94, line 12 - p. 95, line 9) and a block permission table for accessing a

permission table that describes memory access control information (*Specification*, p. 100, line 23 - p. 101, line 16). Performing an integrity check of the revocation list and the block permission table (*Specification*, p. 102, lines 6-21).

Independent claim 31 recites a computer-readable medium comprising a computer program product for performing, when executed by a processor, a data encryption method comprising storing data in a memory having a data storage area consisting of a plurality of blocks, each of the blocks consists of M sectors from a first sector to a M-th sector with each sector having a predetermined data capacity, where M represents a natural number (*Specification*, p. 108, lines 7-10 and p. 112, lines 13-24). Encryption processing data to be stored in the sectors by performing encryption using a different encryption key for each sector from the first sector to the M-th sector (*Specification*, p. 108, lines 7-13). Storing data including a revocation list having revocation information regarding revoked media or content (*Specification*, p. 106, line 11 p. 107, line 15) and a block permission table for accessing a permission table that describes memory access control information (*Specification*, p. 113, lines 2-10). Checking the integrity of the revocation list and the block permission table. (*Specification*, p. 113, lines 11-16).

Independent claim 32 recites a computer readable medium comprising a computer program product for performing, when executed by a processor, a data decryption method comprising reading data from a memory having a data storage area consisting of a plurality of blocks, each of the blocks consists of M sectors from a first sector to a M-th sector with each sector having a predetermined data capacity, where M represents a natural number (*Specification*, p. 93, lines 10-21). Decrypting data stored



in each of the sectors by executing decryption processing using a different decryption key for each sector from the first sector to the M-th sector (*Specification*, p. 96, lines 19-25). Storing data including a revocation list having revocation information regarding revoked media or content (*Specification*, p. 94, line 12 - p. 95, lines 9) and a block permission table for accessing a permission table that describes memory access control information (*Specification*, p. 100, line 23 - p. 101, line 16). Checking the integrity of the revocation list and the block permission table. (*Specification*, p. 102, lines 6-21).

#### VI. Grounds of Rejection

Claims 1, 2, 5, 8, 9, 12, 15-18, 21, 24, 25, 28, 31, and 32 stand rejected under 35 U.S.C. 103(a) as being unpatentable over *Hazard* (U.S. Patent No. 6,658,566) in view of *Sudia* (Published U.S. Patent Application No. 2005/0114666).<sup>1</sup>

Claims 3, 4, 6, 10, 11, 13, 19, 20, 22, 26, 27, and 29 stand rejected under 35 U.S.C. 103(a) as being unpatentable over *Hazard* in view of *Sudia* and further in view of *Dilkie et al.* (U.S. Patent No. 6,341, 164).

Claims 7, 14, 23, and 30 stand rejected under 35 U.S.C. 103(a) as being unpatentable over *Hazard* in view of *Sudia* and further in view of "Applied Cryptography" by *Schneier*.

#### VII. Arguments

Appellants respectfully request the Board to reverse the Examiner's rejections of claims 1, 5, 6, 8, 12, 13, 15-17, 21, 22, 24, 28, 29, 31, and 32.

---

<sup>1</sup> The Examiner failed to include claims 9 and 12 in the heading of the rejection. However, based on the body of the rejection, it appears that claims 9 and 12 were intended to be included.

A. The Subject Matter of the Claimed Invention Would Not Have  
Been Obvious in view of *Hazard* and *Sudia*

*Hazard* and *Sudia*, taken alone or in any reasonable combination, fail to teach or disclose all the limitations of independent claims 1, 8, 15, 17, 24, 31, and 32.

The recording device of claim 1 protects stored data by encrypting the data in each of a plurality of sectors with a different encryption key. (*Specification*, p. 39, lines 19-25.) The term “sector” refers to an allocated area of a storage medium that is used by file management systems, such as a file allocation table (FAT), to store and retrieve data. (*Id.* at p. 2, line 23 - p. 3, line 6.) In the FAT system, the storage medium is divided into blocks (clusters), which are further divided into sectors. (*Id.* at p. 3, lines 2-6 and Fig. 3.) For example, one block may comprise 32 sectors and each sector may comprise 512 bytes. (*Id.* at p. 40, line 7 and p. 87, lines 1-10.) When a file is stored in memory, the FAT system divides each file based on the sector size of the memory, and stores the file across multiple sectors. (*Id.* at p. 3, lines 2-4.) For example, if a file has a size of 1536 bytes, the FAT system may divide the file into three pieces consisting of 512 bytes and store those three pieces into three sectors.

Conversely to sector level encryption, *Hazard* discloses data encryption at the file level. In particular, *Hazard* discloses a process of protecting sensitive information stored on a security module by encrypting the sensitive information using a temporary protection key. (*Hazard*, 1:62-66.) The sensitive information may be “a bank account number, a message, or even an entire document.” (*Id.* at 1:35-38.) *Hazard* further discloses “several temporary encrypting protection keys CP1, ... CPi, ... Cpn and several associated temporary decrypting protection keys CPd1, ... CPdi, ... CPdn.” (*Id.*

at 4:32-35.) The relationship between the temporary encrypting protection keys (CP) and the sensitive information (IS) is illustrated in the tables of FIGs. 2 and 3 of *Hazard*.

As set forth by *Hazard*:

[t]he table of FIG. 3 includes, in a first column, references to a number *m* of items of sensitive information IS<sub>1</sub>, IS<sub>2</sub>,... IS<sub>(j-1)</sub>, IS<sub>j</sub>, ... IS<sub>m</sub>, each of which is stored in the security module in encrypted form using an encryption algorithm and a temporary protection key chosen from among those in table of FIG. 2. A second column in the table defines the number of the temporary protection key used for each item of sensitive information. (*Id.* at 5:15-22.)

FIG. 3 indicates that sensitive information IS<sub>1</sub> and IS<sub>2</sub> are encrypted with the encryption key associated with key number "N1." (*Id.*) FIG. 2 indicates that the encryption key associated with key number "N1" is "CP1." (*Id.* at 5:22-24.) This does not equate to "us[ing] a different encryption key for each sector from the first sector to the M-th sector," as recited in independent claims 1, 8, 17, and 31. It also does not equate to "us[ing] a different decryption key for each sector from the first sector to the M-th sector," as recited in independent claims 24 and 32. Instead, *Hazard* discloses the use of a temporary protection key based upon the sensitive information (IS) and not based upon a sector. The entire sensitive information (IS) is encrypted using "an encryption algorithm and a temporary protection key chosen from among those in the table of FIG. 2." (*Id.* at 5:18-20)(emphasis added.) In other words, each sensitive information (IS) is encrypted with one encryption key.

Moreover, an interpretation of the different sensitive information disclosed by *Hazard* as the claimed sector still does not lead to or suggest the claimed information recording device. As recited in independent claims 1, 8, 17, 24, 31, and 32, "a different

encryption key is used for each sector.” As discussed above, sensitive information IS1 and IS2 of *Hazard* is encrypted using the same encryption key, “CP1.”

*Sudia* fails to cure the above deficiencies of *Hazard*. Instead, the Examiner relies on *Sudia* for the teaching of “data includ[ing] a revocation list having revocation information regarding revoked media or content,” as recited in independent claims 1, 8, 15, 17, 24, 31, and 32. Specifically, the Examiner cites the “revocation info” disclosed by *Sudia*. (See e.g., *Final Office Action*, p. 3.)

*Sudia* discloses a method to secure digital certificates to ensure that a user of the digital certificate is authorized to use the digital certificate for a particular transaction. (*Sudia*, ¶ 4.) A user’s level of authorization is contained within the digital certificate in the form of hash values (i.e., a randomized string of data). (*Id.* at ¶ 228.) *Sudia* further discloses “revocation info” to manage changes to a user’s granted authorizations. (*Id.* at ¶ 244.) For example, if a particular authorization of a user is revoked, instead of revoking and reissuing a new digital certificate, the certificate instead includes a “revocation info” field which contains revoked authorizations. (*Id.*) Prior to conducting a transaction, a relying party may electronically check the “revocation info” field to determine if the user is still authorized to conduct the transaction. (*Id.* at ¶ 245.) Thus, the “revocation info” field pertains to a user’s authorization. It does not equate to a “revocation list having revocation information regarding revoked media or content,” as recited in independent claims 1, 8, 15, 17, 24, 31, and 32.

Nevertheless, the Examiner further asserts this position stating, “revoked privileges are associated with content that the user may no longer access based on the revocation, hence revocation information regarding revoked content (par. 362).”

(*Advisory Action*, p. 2.) Appellants respectfully disagree with the Examiner's assertion. *Sudia* discloses privileges and authorizations that are granted to and revoked from a user. The privileges and authorizations are not granted to and revoked from media or content. Specifically, under the system of *Sudia*, a user's "access to the content [is] governed by a given privilege." (*Sudia*, at ¶ 362.) For example, if a first user's privilege is revoked, the first user may not access the content, while a second user, whose privilege is not revoked, is free to access the content. On the contrary, if the revocation is "regarding revoked media or content," then neither the first nor the second user would have access to the content. Accordingly, the revoked privileges and authorizations do not constitute "revoked media or content," as recited in claims 1, 8, 15, 17, 24, 31, and 32.

Further, *Hazard* and *Sudia* also fail to disclose a "block permission table for accessing a permission table that describes memory access control information," as recited in claims 1, 8, 15, 17, 24, 31, and 32. According to the Examiner, this recitation "is nothing more than a table that leads to various user rights to various elements stored in memory." (*Advisory Action*, p. 2.) Appellants respectfully disagree. The block permission table does not "lead[s] to various user rights," as asserted by the Examiner. (*Id.*) Instead, it accesses a "permission table that describes memory access control information." For example, for each block unit of the memory, the block permission table specifies the type of processing permitted, such as "a block that can be erased, a block that cannot be erased, a block that can be played back, and a block that cannot be played back." (*Specification*, p. 45, lines 14 -16.)

Nowhere in *Hazard* or *Sudia* is there a disclosure of the claimed “block permission table.” Indeed, aside from the Examiner’s conclusory statement in the Advisory Action, the Examiner fails to provide any showing of support for such conclusion in either reference.

Independent claims 1, 8, 15, 17, and 24 further recite an “integrity checking unit for checking the integrity of the revocation list and the block permission table.” Similarly, independent claims 31 and 32 recite, “checking the integrity of the revocation list and the block permission table.” The Examiner admits that *Hazard* and *Sudia* do “not explicitly disclose[d] [is] checking the integrity of the revocation list and checking the integrity of the block permission table.” (*Final Office Action*, p. 4.) Nevertheless, the Examiner concludes:

[h]owever, *Sudia* et al. teach that it is important to check the integrity of the information in the tables that ultimately allow users’ access to resources in order to ensure that the permissions/revocation list is being enforced in such a way that a user exceeds their permissions/resources that they should be able to access. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in *Hazard* et al. to have an integrity unit in order to ensure the integrity of the revocation list and block permission table. (*Id.*)

The Examiner contends that support for this conclusion can be found in paragraphs 362 and 363 of *Sudia*. (*Advisory Action*, p. 2.) However, the cited paragraphs are directed towards verifying that a user has “access to the content governed by a given privilege.” (*Sudia*, ¶ 362.) *Sudia* does not disclose checking “the integrity of the revocation list and the block permission table.”

Thus, even if *Hazard* were combined with *Sudia* as the Examiner suggests, *Hazard* and *Sudia* do not disclose all the elements recited in independent claims 1, 8,

15, 17, 24, 31, and 32. For at least this reason, the cited prior art fails to establish a *prima facie* case of obvious regarding independent claims 1, 8, 15, 17, 24, 31, and 32. Accordingly, Appellants respectfully request that the rejection of these claims under 35 U.S.C. § 103(a) be reversed by the Board.

B. Claims 5, 12, 16, 21, and 28 Patentably Distinguish Over *Hazard* and *Sudia*

Claims 5, 12, 16, 21, and 28 depend from claims 1, 8, 15, 17, and 24, respectively. As explained, claims 1, 8, 15, 17, and 24 are distinguishable from *Hazard* and *Sudia*. Accordingly, claims 5, 12, 16, 21, and 28 are also distinguishable from these references for at least the same reason set forth above in connection with claims 1, 8, 15, 17, and 24. Therefore, Appellants respectfully request that the Board reverse the rejection of these claims under 35 U.S.C. § 103(a).

C. *Dilkie et al.* Does Not Cure the Deficiencies of *Hazard* and *Sudia*

With respect to dependent claims 6, 13, 22, and 29, as demonstrated above, *Hazard* in view of *Sudia* fail to teach or suggest all the elements of independent claims 1, 8, 15, 17, and 24. Further, the Examiner does not rely upon, nor does *Dilkie et al.* disclose the deficiencies of *Hazard* and *Sudia* discussed above. Accordingly, at least for the reason that claims 6, 13, 22, and 29 depend from independent claims 1, 8, 15, 17, and 24, Appellants respectfully request that the Board reverse the rejection of these claims under 35 U.S.C. § 103(a).

D. The Rejection of Claims 2-4, 7, 9-11, 14, 18-20, 23, 25-27, and 30 are Rendered Moot

Appellants file concurrently with this Appeal Brief an Amendment pursuant to 37 C.F.R. §§ 1.116 and 41.33(b) proposing to cancel claims 2-4, 7, 9-11, 14, 18-20, 23,

25-27, and 30. Upon entry of the amendment, the rejection of these claims under 35 U.S.C. § 103(a) will be rendered moot.

E. Conclusion


For the reasons above, pending claims 1, 5, 6, 8, 12, 13, 15-17, 21, 22, 24, 28, 29, 31, and 32 are allowable and reversal of the Examiner's rejection is respectfully requested.

To the extent any extension of time under 37 C.F.R. § 1.136 is required to obtain entry of this Appeal Brief, such extension is hereby respectfully requested. If there are any fees due under 37 C.F.R. §§ 1.16 or 1.17 which are not enclosed herewith, including any fees required for an extension of time under 37 C.F.R. § 1.136, please charge such fees to our Deposit Account No. 06-0916.

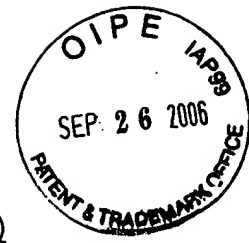
Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,  
GARRETT & DUNNER, L.L.P.

Dated: September 26, 2006

By:   
Arthur A. Smith  
Reg. No. 56,877





VIII. Claims Appendix to Appeal Brief Under Rule 41.37(c)(1)(viii)

1. An information recording device for executing processing which stores data to a memory having a data storage area consisting of a plurality of blocks, each of the blocks consists of M sectors from a first sector to a M-th sector with each sector having a predetermined data capacity, where M represents a natural number, said information recording device comprising:

a cryptosystem unit that selectively uses a different encryption key for each sector from the first sector to the M-th sector to execute encryption processing and the cryptosystem unit executes encryption processing on data to be stored in each of the sectors;

wherein the data includes a revocation list having revocation information regarding revoked media or content and a block permission table for accessing a permission table that describes memory access control information; and

an integrity checking unit for checking the integrity of the revocation list and the block permission table.

5. An information recording device according to claim 1, wherein, in said cryptosystem unit, the encryption processing for the first sector to the M-th sector is executed as single-DES encryption processing using different encryption keys for the sectors.

6. An information recording device according to claim 1, wherein, in said cryptosystem unit, the encryption processing for the first sector to the M-th sector is

executed as triple-DES encryption processing using at least two different encryption keys for each of the sectors.

8. An information playback device for executing processing which reads data from a memory having a data storage area consisting of a plurality of blocks, each of the blocks consists of M sectors from a first sector to a M-th sector with each sector having a predetermined data capacity, where M represents a natural number said information playback device comprising:

a cryptosystem unit which selectively uses a different decryption key for each sector from the first sector to the M-th sector to execute decryption processing and the cryptosystem unit executes decryption processing on data stored in each of the sectors;

wherein the data includes a revocation list having revocation information regarding revoked media or content and a block permission table for accessing a permission table that describes memory access control information; and

an integrity checking unit for checking the integrity of the revocation list and the block permission table.

12. An information playback device according to claim 8, wherein, in said cryptosystem unit, the decryption processing for the first sector to the M-th sector is executed as single-DES decryption processing using different decryption keys for the sectors.

13. An information playback device according to claim 8, wherein, in said cryptosystem unit, the decryption processing for the first sector to the M-th sector is executed as triple-DES decryption processing using at least two different decryption keys for each of the sectors.

15. An information recording medium having a data storage area consisting of a plurality of blocks, each of the blocks consists of M sectors from a first sector to a M-th sector with each sector having a predetermined data capacity, where M represents a natural number,

wherein a plurality of different cryptographic keys which are selectable for the sectors are stored as header information of data stored in said data storage area,

wherein the storage area stores data including a revocation list having revocation information regarding revoked media or content and a block permission table for accessing a permission table that describes memory access control information, and

wherein an integrity check of the integrity of the revocation list and block permission table is performed.

16. An information recording medium according to claim 15, wherein said plurality of different cryptographic keys are M different encryption keys corresponding to the M sectors.

17. An information recording method for executing processing which stores data to a memory having a data storage area consisting of a plurality of blocks, each of

the blocks consists of M sectors from a first sector to a M-th sector with each sector having a predetermined data capacity, where M represents a natural number, said information recording method comprising:

encryption processing data to be stored in the sectors by performing encryption using a different encryption key for each sector from the first sector to the M-th sector;

storing data including a revocation list having revocation information regarding revoked media or content and a block permission table for accessing a permission table that describes memory access control information; and

performing an integrity check of the revocation list and the block permission table.

21. An information recording method according to claim 17, wherein the encryption processing is executed as single-DES encryption processing using different encryption keys for the sectors.

22. An information recording method according to claim 17, wherein the encryption processing is executed as triple-DES encryption processing using at least two different encryption keys for each of the sectors.

24. An information playback method for executing processing which reads data from a memory having a data storage area consisting of a plurality of blocks, each of the blocks consists of M sectors from a first sector to a M-th sector with each sector

having a predetermined data capacity, where  $M$  represents a natural number, said information playback method comprising:

decrypting data stored in each of the sectors by executing decryption processing using a different decryption key for each sector from the first sector to the  $M$ -th sector;

storing data including a revocation list having revocation information regarding revoked media or content and a block permission table for accessing a permission table that describes memory access control information; and

performing an integrity check of the revocation list and the block permission table.

28. An information playback method according to claim 24, wherein the decryption processing is executed as single-DES decryption processing using different decryption keys for the sectors.

29. An information playback method according to claim 24, wherein the decryption processing is executed as triple-DES decryption processing using at least two decryption keys for each of the sectors.

31. A computer-readable medium comprising a computer program product for performing, when executed by a processor, a data encryption method comprising:

storing data in a memory having a data storage area consisting of a plurality of blocks, each of the blocks consists of  $M$  sectors from a first sector to a  $M$ -th sector with

each sector having a predetermined data capacity, where M represents a natural number;

encryption processing data to be stored in the sectors by performing encryption using a different encryption key for each sector from the first sector to the M-th sector;

storing data including a revocation list having revocation information regarding revoked media or content and a block permission table for accessing a permission table that describes memory access control information; and

checking the integrity of the revocation list and the block permission table.

32. A computer readable medium comprising a computer program product for performing, when executed by a processor, a data decryption method comprising:

reading data from a memory having a data storage area consisting of a plurality of blocks, each of the blocks consists of M sectors from a first sector to a M-th sector with each sector having a predetermined data capacity, where M represents a natural number;

decrypting data stored in each of the sectors by executing decryption processing using a different decryption key for each sector from the first sector to the M-th sector;

storing data including a revocation list having revocation information regarding revoked media or content and a block permission table for accessing a permission table that describes memory access control information; and

checking the integrity of the revocation list and the block permission table.

IX. Evidence Appendix to Appeal Brief Under Rule 41.37(c)(1)(ix)

Appellants do not rely on any evidence in this Appeal.

X. Related Proceedings Appendix to Appeal Brief Under Rule 41.37(c)(1)(x)

To Appellants' knowledge, there are no related proceedings or decisions.